

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-115413

(43)公開日 平成7年(1995)5月2日

(51)Int.Cl.<sup>5</sup>H 0 4 L 9/00  
9/10  
9/12

識別記号

庁内整理番号

F I

技術表示箇所

7304-5K

H 0 4 L 9/ 00

Z

H 0 4 B 7/ 26

1 0 9 S

審査請求 有 請求項の数 2 F D (全 7 頁) 最終頁に続く

(21)出願番号 特願平5-282089

(22)出願日 平成5年(1993)10月18日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 白澤 進

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 蒲池 健一郎

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 友池 裕元

東京都港区芝五丁目7番1号 日本電気株式会社内

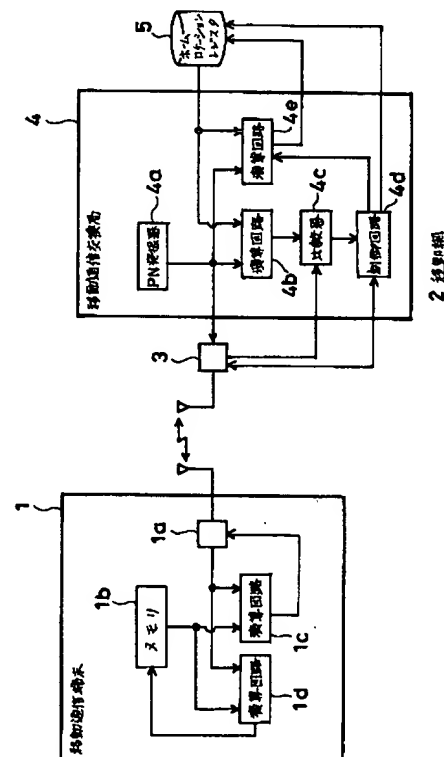
(74)代理人 弁理士 山川 政樹

(54)【発明の名称】 移動通信端末認証方式

(57)【要約】

【目的】 認証キーを端末と移動網間で伝送することなく更新させて移動通信システムの不正利用を防止する。

【構成】 PN発振器4aから送信された乱数及びメモリ1bからの認証キーに基づく演算Fが演算回路1cで行われ、演算結果が移動網2に送信される。この演算結果と演算回路4bにて乱数及びホームロケーションレジスタ5からの認証キーに基づく演算Fが行われた結果とが比較器4cで比較される。比較結果が一致すると認証キー更新指示が制御回路4dから移動通信端末1に送信される。演算回路1dで乱数及び認証キーに基づく演算Gが行われ、新たな認証キーとしてメモリ1bに記憶される。演算回路4eにおいても同様に演算Gが行われてレジスタ5の認証キーが更新される。



## 【特許請求の範囲】

【請求項 1】 移動通信システムの移動通信端末と移動網で同一の認証キーを記憶し、端末の正当性を確認する認証処理のための乱数を移動網から移動通信端末に送信する移動通信端末認証方式において、

受信した乱数及び記憶している認証キーに基づく第 1 の演算を行ってこの結果を送信し、認証キー更新指示を受信すると前記乱数及び認証キーに基づく第 2 の演算を行ってこの結果を新たな認証キーとして記憶する移動通信端末と、

前記乱数を生成して移動通信端末に送信すると共に前記乱数及び記憶している認証キーに基づく第 1 の演算を行い、この結果と移動通信端末から送信された結果が一致したときは、移動通信端末に認証キー更新指示を送信すると共に前記乱数及び認証キーに基づく第 2 の演算を行ってこの結果を新たな認証キーとして記憶する移動網とを有することを特徴とする移動通信端末認証方式。

【請求項 2】 請求項 1 記載の移動通信端末認証方式において、

移動通信端末は、移動網と通信を行うための無線送受信機と、

認証キーを記憶するメモリと、

無線送受信機を介して受信した乱数及びメモリから出力された認証キーに基づく第 1 の演算を行いこの結果を無線送受信機に出力する第 1 の演算回路と、

無線送受信機を介して認証キー更新指示を受信すると前記乱数及び認証キーに基づく第 2 の演算を行いこの結果を新たな認証キーとしてメモリに記憶させる第 2 の演算回路とを有し、

移動網は、前記移動通信端末と通信を行うための無線基地局と、

認証キーを記憶するホームロケーションレジスタと、

交換接続を行う移動通信交換局とを有し、

この移動通信交換局は、前記乱数を生成して無線基地局に出力する発振器と、前記乱数及びホームロケーションレジスタから出力された認証キーに基づく第 1 の演算を行う第 3 の演算回路と、この第 3 の演算回路の結果と無線基地局を介して移動通信端末より受信した演算結果を比較する比較器と、この比較結果が一致したときは認証キー更新指示を無線基地局に出力する制御回路と、前記比較結果が一致したときは前記乱数及び認証キーに基づく第 2 の演算を行いこの結果を新たな認証キーとしてホームロケーションレジスタに記憶させる第 4 の演算回路とを備えることを特徴とする移動通信端末認証方式。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、移動通信システムにおいて、移動網との間で通信を行おうとする移動通信端末が移動網に登録された正当な端末であることを確認するための移動通信端末認証方式に関する。

## 【0002】

【従来の技術】移動通信方式では、移動通信端末が無線回線で移動網と接続されているので、不正な移動通信端末による不正使用を防止し正当な端末に通信料の課金を行うためには、移動網に対して通信を要求する移動通信端末が移動網に登録された正当な端末であるかどうかを確認する認証処理が必要となる。

【0003】図 3 は従来の移動通信端末認証方式を利用した移動通信システムのブロック図である。11 は移動通信端末、11a は移動網と通信を行うための無線送受信機、11b は不正使用を防止するための暗証番号に相当する認証キーを記憶しているメモリ、11c は認証キーと後述する乱数に基づき演算処理を行う演算回路である。

【0004】また、12 は移動通信端末 11 が契約している移動網、13 は移動通信端末 11 と通信を行うための無線基地局、14 は例えば移動通信端末 11 と他の固定網との交換接続を行う移動通信交換局、14a は認証処理のための乱数を通信の度に生成する PN 発振器、14b は PN 発振器 14a から出力された乱数と後述するホームロケーションレジスタに記憶されている認証キーに基づき演算処理を行う演算回路、14c は演算回路 14b の結果と無線基地局 13 を介して移動通信端末 11 より受信した演算結果を比較する比較器、14d は比較器 14c の結果に基づいて呼接続処理などを行う制御回路である。

【0005】また、15 は例えば他の移動通信交換局（ホームメモリ局）に設置されたホームロケーションレジスタであり、移動通信端末 11 の契約加入者情報、呼処理情報等を記憶しており、また移動通信端末 11 のメモリ 11b に記憶されている認証キーと同一な認証キーを移動通信端末 11 に対応づけて記憶している。そして、移動通信交換局 14 は、移動通信端末 11 からの通信の要求に対してホームロケーションレジスタ 15 にアクセスして移動通信端末 11 に関するサービス情報、呼処理情報、認証情報等を取得することができる。

【0006】次に、このような移動通信システムにおいて移動通信端末 11 が正当な端末かどうかを確認する認証処理の動作を説明する。まず、移動通信端末 11 が移動網 12 に対して発信要求を送信すると、無線基地局 13 を介してこの発信要求を受信した移動通信交換局 14 は、その内部の PN 発振器 14a に乱数を発生させる。そして、この乱数は無線基地局 13 から移動通信端末 11 に送信される。

【0007】次いで、移動通信端末 11 内の無線送受信機 11a は、移動網 12 から送信された乱数を受信して演算回路 11c に出力する。演算回路 11c はこの乱数とメモリ 11b に記憶されている認証キーに基づいて演算を行い、無線送受信機 11a はこの結果を移動網 12 に送信する。

## 3

【0008】一方、移動通信交換局14内の演算回路14bは、先にPN発振器14aから出力された乱数とホームロケーションレジスタ15に記憶されている移動通信端末11の認証キーに基づき演算回路11cと同一のアルゴリズムの演算を行う。そして、比較器14cは、移動通信端末11から送信された演算結果と演算回路14bから出力された演算結果を比較する。

【0009】この比較器14cによる比較の結果2つの演算結果が一致すれば、制御回路14dは、正当な端末と判定して移動通信端末11と呼接続処理を行い、不一致であれば不正な端末と判定して呼接続処理を拒絶する。これで、認証処理が終了する。

【0010】上記の移動通信端末認証方式は、記憶している同一の認証キーを同一の演算アルゴリズムを有する演算回路11c、14bでそれぞれ演算処理してこれらの結果を移動網12側で比較し、移動通信端末11の正当性を判定するという認証方式である。しかし、移動通信端末11と移動網12で共有している認証キー、演算回路を不正にコピーした移動通信端末を作ったとすると、上記認証方式では移動通信端末11の真偽を移動通信交換局14で認識することができなくなる。

【0011】そこで、特開平2-224425号公報で開示された移動通信方式は、通信の度ごとに次回使用する認証キーを送信し、移動網と移動通信端末双方で通信の度ごとに認証キーを更新して保持しておく認証方式となっている。この方式によれば認証キーを含めた移動通信端末がコピーされると、不正端末が通信を行った際に移動網側で認証キーが更新されて正規の端末の認証キーとの不一致が生じる。よって、次に正規の端末が通信を行う際に不一致となるので、正規の加入者は不正端末が存在することを早期に発見し、契約している移動網に申告し認証キーを再度設定することで一時的にこの不正端末を排除できる。

【0012】しかし、この移動通信方式では次回使用する認証キーを移動網から移動通信端末に対して無線回線で送信するため、不正端末が移動網から送信された回目の認証キーを再度傍受することができれば認証キーを更新することができ、その不正端末は再度不正に移動通信サービスを受けることができてしまう。

【0013】

【発明が解決しようとする課題】従来の移動通信端末認証方式は以上のようにして認証処理を行っていたので、記憶している同一の認証キーを演算処理してその結果を照合することにより端末の正当性を判定する認証方式では、認証キー及び演算回路をコピーした不正な端末が存在しても移動網側でその存在を認識できないという問題点があった。また、移動網と移動通信端末双方で通信の度ごとに認証キーを更新する認証方式では、次回使用する認証キーを移動網から端末に対して送信するので、一時的に不正端末を排除できても不正端末が次の認証キ

## 4

一を傍受すると、その不正端末は再度移動通信サービスを受けることができてしまうという問題点があった。本発明は、上記課題を解決するために、端末と移動網で記憶している認証キーを伝送せずに更新させて移動通信システムの不正利用を防止することができる移動通信端末認証方式を提供することを目的とする。

【0014】

【課題を解決するための手段】本発明は、受信した乱数及び記憶している認証キーに基づく第1の演算を行ってこの結果を送信し、認証キー更新指示を受信すると乱数及び認証キーに基づく第2の演算を行ってこの結果を新たな認証キーとして記憶する移動通信端末と、乱数を生成して移動通信端末に送信すると共に乱数及び記憶している認証キーに基づく第1の演算を行い、この結果と移動通信端末から送信された結果が一致したときは、移動通信端末に認証キー更新指示を送信すると共に乱数及び認証キーに基づく第2の演算を行ってこの結果を新たな認証キーとして記憶する移動網とを有するものである。

【0015】また、移動通信端末は、移動網と通信を行うための無線送受信機と、認証キーを記憶するメモリと、無線送受信機を介して受信した乱数及びメモリから出力された認証キーに基づく第1の演算を行いこの結果を無線送受信機に出力する第1の演算回路と、無線送受信機を介して認証キー更新指示を受信すると乱数及び認証キーに基づく第2の演算を行いこの結果を新たな認証キーとしてメモリに記憶させる第2の演算回路とを有し、移動網は、移動通信端末と通信を行うための無線基地局と、認証キーを記憶するホームロケーションレジスタと、交換接続を行う移動通信交換局とを有し、この移動通信交換局は、乱数を生成して無線基地局に出力する発振器と、乱数及びホームロケーションレジスタから出力された認証キーに基づく第1の演算を行う第3の演算回路と、この第3の演算回路の結果と無線基地局を介して移動通信端末より受信した演算結果を比較する比較器と、この比較結果が一致したときは認証キー更新指示を無線基地局に出力する制御回路と、比較結果が一致したときは乱数及び認証キーに基づく第2の演算を行いこの結果を新たな認証キーとしてホームロケーションレジスタに記憶させる第4の演算回路とを備えるものである。

【0016】

【作用】本発明によれば、移動網から乱数が送信され、移動通信端末にて受信した乱数及び記憶している認証キーに基づく第1の演算が行われて移動網に送信され、この演算結果と移動網の内部で乱数及び認証キーに基づく第1の演算が行われた結果とが比較される。そして、この比較結果が一致すると移動網から認証キー更新指示が送信され、移動通信端末にて乱数及び認証キーに基づく第2の演算が行われてこの結果が新たな認証キーとして記憶されると共に、移動網においても同様に第2の演算が行われて認証キーが更新される。

## 5

【0017】また、無線基地局を介して発振器から乱数が送信され、受信した乱数及びメモリで記憶している認証キーに基づく第1の演算が第1の演算回路にて行われて無線送受信機を介して移動網に送信され、この演算結果と第3の演算回路にて乱数及びホームロケーションレジスタからの認証キーに基づく第1の演算が行われた結果とが比較器で比較される。そして、この比較結果が一致すると認証キー更新指示が制御回路から無線基地局を介して移動通信端末に送信され、第2の演算回路にて乱数及び認証キーに基づく第2の演算が行われてこの結果が新たな認証キーとしてメモリに記憶されると共に、第4の演算回路においても同様に第2の演算が行われてホームロケーションレジスタの認証キーが更新される。

【0018】

【実施例】図1は本発明の1実施例を示す移動通信端末認証方式を利用した移動通信システムのブロック図、図2はこの移動通信端末認証方式における認証処理の手順を示す図である。

【0019】図1において、1は移動通信端末、1aは無線送受信機、1bは電源断時も内容を記憶している不揮発メモリであって認証キーを記憶しているメモリ、1cは図3の演算回路11cと同様に受信した乱数とメモリ1bに記憶された認証キーに基づいて第1の演算を行う第1の演算回路、1dは無線送受信機1aを介して認証キー更新指示を受信すると乱数及び認証キーに基づく第2の演算を行いこの結果を新たな認証キーとしてメモリ1bに記憶させる第2の演算回路である。

【0020】また、3は無線基地局、4は移動通信交換局、4aはPN発振器、4bは演算回路14bと同様にPN発振器4aから出力された乱数とホームロケーションレジスタに記憶されている認証キーに基づいて第1の演算を行う第3の演算回路、4cは第3の演算回路4bの結果と無線基地局3を介して移動通信端末1より受信した演算結果を比較する比較器である。

【0021】また、4dは比較器4cによる比較結果が一致したときは認証キー更新指示を無線基地局3に出力して移動通信端末1に送信させる制御回路、4eは上記の比較結果が一致したときは乱数及び認証キーに基づく第2の演算を行いこの結果を新たな認証キーとしてホームロケーションレジスタに記憶させる第4の演算回路、5は図3の例と同様のホームロケーションレジスタである。

【0022】図2において、 $P1n$ 、 $P2n$ はそれぞれホームロケーションレジスタ5、メモリ1bに記憶されている認証キー、 $Rn$ はPN発振器4aで生成された乱数、 $C1n$ 、 $C2n$ はそれぞれ第3の演算回路4b、第1の演算回路1cによる第1の演算Fの結果、 $P1n+1$ 、 $P2n+1$ はそれぞれ第4の演算回路4e、第2の演算回路1dによる第2の演算Gの結果得られた新しい認証キーである。また、 $F(P1n, Rn)$ は認証キーP

## 6

$1n$ と乱数 $Rn$ に基づく第1の演算Fを示し、 $G(P1n, Rn)$ は同じく第2の演算Gを示す。

【0023】次に、このような移動通信システムにおいて移動通信端末1が正当な端末かどうかを確認する認証処理の動作を説明する。まず、移動通信端末1からの発信要求を受信した移動通信交換局4は、制御回路4dによって移動通信端末1に関する呼処理情報を蓄積しているホームロケーションレジスタ5にアクセスし、発信要求の中に含まれる移動通信端末1の移動機番号(MS I: Mobile Station Identity)で発信情報読み出しを要求する。

【0024】そして、この要求に対する発信情報読み出し応答としてホームロケーションレジスタ5から出力された移動通信端末1の認証キー $P1n$ を受け取ると共に、PN発振器4aに乱数 $Rn$ を発生させる。この乱数 $Rn$ は無線基地局3から移動通信端末1に送信される。また、演算回路4bは、PN発振器4aから出力された乱数 $Rn$ とホームロケーションレジスタ5から読み出された移動通信端末1の認証キー $P1n$ に基づき演算Fを実行してこの結果 $C1n$ を比較器4cに出力する。

【0025】次に、移動通信端末1内の無線送受信機1aは、移動網2から送信された乱数 $Rn$ を受信して演算回路1cに出力する。演算回路1cは、この乱数 $Rn$ とメモリ1bに記憶されている認証キー $P2n$ に基づき演算Fを実行してこの結果 $C2n$ を無線送受信機1aに出力する。この演算結果 $C2n$ は無線送受信機1aから移動網2に送信される。

【0026】そして、移動通信交換局4内の比較器4cは、演算回路4bから出力された演算結果 $C1n$ と移動通信端末1から送信され無線基地局3が受信した演算結果 $C2n$ を比較し、移動通信端末1の正当性を判定する。このとき、移動通信端末1が正規の端末であればホームロケーションレジスタ5が記憶している認証キー $P1n$ と端末1が記憶している認証キー $P2n$ は同じはずであり、演算回路4b、1cによる演算アルゴリズムも第1の演算Fで同一なので、演算結果 $C1n$ と $C2n$ も等しいはずである。

【0027】よって、移動通信交換局4内の制御回路4dは、比較器4cによる比較の結果2つの演算結果 $C1n$ 、 $C2n$ が一致すれば正当な端末と判定し、無線基地局3に移動通信端末1に対して認証キー更新指示を送信させる。また、比較の結果が不一致であれば不正な端末と判定して認証がNGであったことを送信させる。

【0028】ここまでの動作は図3の例と同様であるが、次に正当な端末と判定された移動通信端末1では、移動網2からの認証キー更新指示を受信することにより、以下のように認証キー $P2n$ の更新を行う。すなわち、演算回路1dは先の乱数 $Rn$ 及びメモリ1bに記憶されている認証キー $P2n$ に基づき演算Gを実行してこの結果 $P2n+1$ をメモリ1bに出力し、メモリ1bは記

憶している認証キー  $P_{2n}$  をこの新たに生成された認証キー  $P_{2n+1}$  に更新する。

【0029】一方、移動通信交換局 4 においても同様に演算回路 4e が乱数  $R_n$  と認証キー  $P_{1n}$  に基づき演算 G を実行してこの結果  $P_{1n+1}$  をホームロケーションレジスタ 5 に認証キー更新要求として出力する。そして、ホームロケーションレジスタ 5 は、記憶している認証キー  $P_{1n}$  をこの新たに生成された認証キー  $P_{1n+1}$  に更新する。これで、認証処理が終了し、移動通信交換局 4 は移動通信端末 1 の発信要求に対する呼接続処理を行う。

【0030】この認証方式では、ホームロケーションレジスタ 5 が記憶している認証キー  $P_{1n}$  と端末 1 内のメモリ 1b が記憶している認証キー  $P_{2n}$  が同じで、演算回路 4e、1d による演算アルゴリズムも第 2 の演算 G で同一なので、新たに生成された認証キー  $P_{1n+1}$ 、 $P_{2n+1}$  も同一となる。そして、次の移動通信端末 1 に対する認証処理には今回の認証処理で更新されたこれらの認証キー  $P_{1n+1}$ 、 $P_{2n+1}$  が使用される。

【0031】したがって、認証キー  $P_{1n}$ 、 $P_{2n}$  は通信の度に更新されるので、認証キー等が全く同等な不正端末を作ったとすると、この不正端末が通信を行った際には移動網 2 側で認証キー  $P_{1n}$  が更新され正規の端末 1 側の認証キー  $P_{2n}$  は更新されない。よって、次に正規の端末 1 が通信を行う際に認証キーが不一致となるので、正規の加入者は不正端末が存在することを早期に発見することができる。

【0032】そして、無線回線でやり取りする主な情報は、PN 発振器 4a で生成された通信の度ごとに变化する乱数  $R_n$  と演算回路 1c による演算結果  $C_{2n}$  であって、不正端末を作るのに必要となる認証キーが直接伝送されることはなく、また新しい認証キーは乱数  $R_n$  を用いた演算 G により生成される。

【0033】よって、ある時点で認証キー等が全く同等な端末を作ったとしても、その後の通信の際に移動網 2 から送信される乱数  $R_n$  を 1 度でも傍受し損なうと、正規の端末 1 の認証キー  $P_{2n}$  とホームロケーションレジスタ 5 の認証キー  $P_{1n}$  が更新されたにも関わらず、不正端末の認証キーは更新されないままとなり、それ以降不正端末の認証キーとホームロケーションレジスタ 5 の認証キー  $P_{1n}$  が一致することは極めて稀である。

【0034】

【発明の効果】本発明によれば、移動通信端末と移動網で記憶している認証キーを通信の度に更新するので、認証キー等が全く同等な不正端末が存在しても、正規の端末が通信を行う際に認証キーの不一致が生じて不正端末が存在することを早期に発見することができる。また、認証キーを直接伝送せずに乱数を用いた第 2 の演算で認証キーを更新するので、乱数を傍受し損なうか又は不正端末の発覚による認証キーの再設定により、以後不正端末の認証キーと移動網の認証キーが一致することは極めて稀であり、不正端末による再度の不正な利用を防止することができる。

【0035】また、移動通信端末を無線送受信機、メモリ、第 1 の演算回路、第 2 の演算回路から構成し、移動網を無線基地局、ホームロケーションレジスタ、並びに発振器、第 3 の演算回路、比較器、制御回路、及び第 4 の演算回路を有する移動通信交換局から構成することにより、移動通信端末と移動網で記憶している認証キーを直接伝送せずに、通信の度に乱数を用いた第 2 の演算で認証キーを更新させる移動通信端末認証方式を実現することができる。

【図面の簡単な説明】

【図 1】本発明の 1 実施例を示す移動通信端末認証方式を利用した移動通信システムのブロック図である。

【図 2】図 1 の移動通信端末認証方式における認証処理の手順を示す図である。

【図 3】従来における移動通信端末認証方式を利用した移動通信システムのブロック図である。

【符号の説明】

1 移動通信端末

1a 無線送受信機

1b メモリ

1c 第 1 の演算回路

1d 第 2 の演算回路

2 移動網

3 無線基地局

4 移動通信交換局

4a PN 発振器

4b 第 3 の演算回路

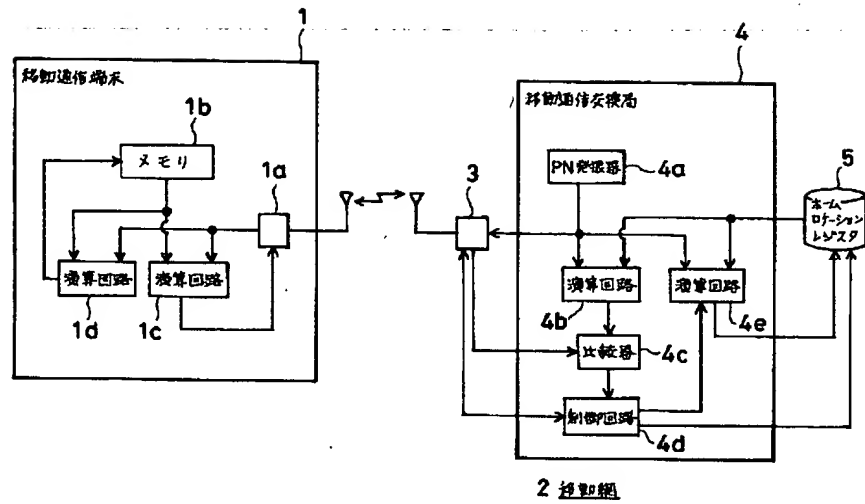
4c 比較器

4d 制御回路

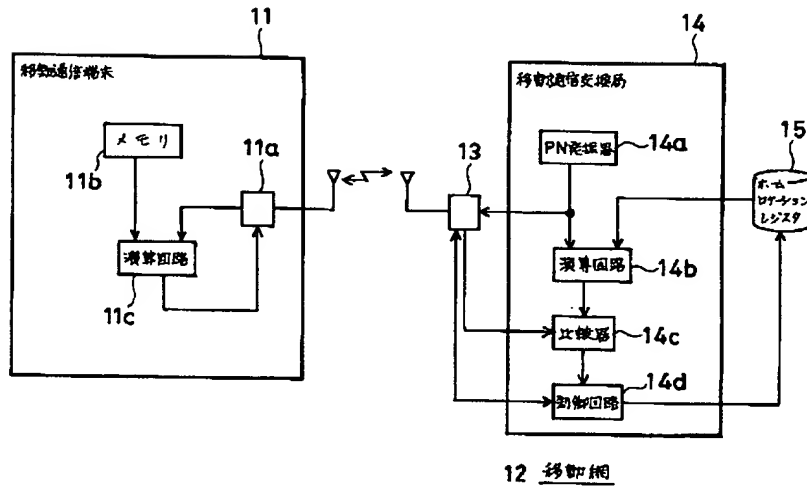
4e 第 4 の演算回路

5 ホームロケーションレジスタ

【図1】

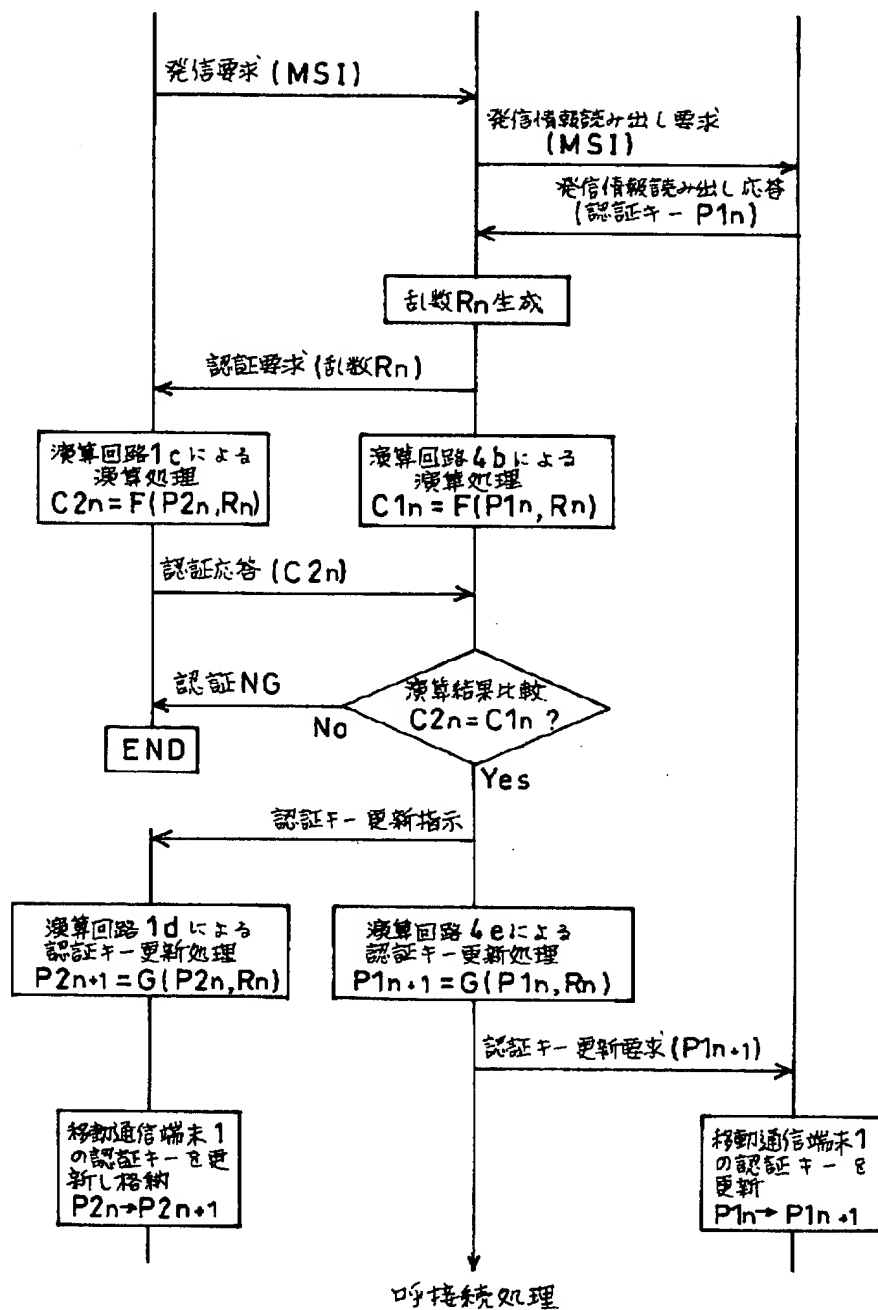


【図3】



【図2】

移動通信端末1      移動通信交換局4      ホームロケーションレジスタ5



フロントページの続き

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.